(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115455398 B
(45)授权公告日 2023.01.10

(21)申请号 202211415792.X

(22)申请日 2022.11.11

(65)同一申请的已公布的文献号
申请公布号 CN 115455398 A

(43)申请公布日 2022.12.09

(73)专利权人 中诚华隆计算机技术有限公司
地址 100012 北京市朝阳区来广营乡紫月路18号院3号楼8层

(72)发明人 王嘉诚 张少仲 张栩

(74)专利代理机构 北京智燃律师事务所 11864
专利代理师 柴琳琳

(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/45(2013.01)
G06F 21/71(2013.01)

(56)对比文件
CN 112041838 A,2020.12.04
CN 108694329 A,2018.10.23
WO 2020013730 A2,2020.01.16
US 2014283107 A1,2014.09.18

审查员 丁文勍

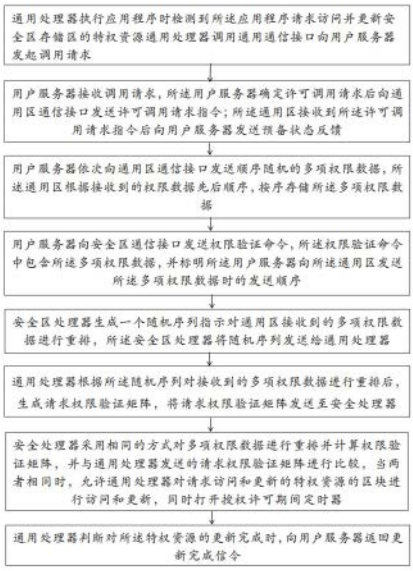
权利要求书3页 说明书9页 附图1页

(54)发明名称

一种基于SoC的物联网终端配置更新方法

(57)摘要

本发明公开了一种基于SoC的物联网终端配置更新方法，涉及计算机技术领域，所述方法包括通用区应用在获得用户服务器的可信许可后，通用区根据服务器送的各项权限数据以及安全区发送的随机序列，生成请求权限验证矩阵向安全区验证后请求对应的特权资源块，安全区根据相同的方式验证后允许通用区对特定区块的特殊资源的访问和更新权限，同时打开定时器，在定时器结束后，终止通用区的上述权限。通过本发明的方法使得通用区不会访问多余不需要的特权数据，也可以防止通用区程序对特权数据做过分的改正更新。



CN 115455398 B

1.一种基于SoC的物联网终端配置更新方法,应用于片上系统SoC,所述SoC包括通用区和安全区,其中所述通用区中包含通用处理器、通用存储区、通用通信接口,所述安全区中包含安全处理器、安全存储区和安全通信接口,所述方法包括:

通用处理器执行应用程序时检测到所述应用程序请求访问并更新安全区存储区的特权资源;

所述通用处理器调用通用通信接口向用户服务器发起调用请求,所述调用请求中包括请求访问并更新的资源内容,以及所述应用程序的信息;

所述用户服务器接收调用请求,所述用户服务器确定许可调用请求后向通用区通信接口发送许可调用请求指令,否则发送拒绝调用请求指令;

所述通用区接收到所述许可调用请求指令后向用户服务器发送预备状态反馈;

所述用户服务器在接收到所述预备状态反馈后,依次向通用区通信接口发送顺序随机的多项权限数据,所述多项权限数据包括:授权许可期间,所述请求访问并更新的特权资源对应的区块ID,所述请求访问并更新的特权资源对应的每一区块的哈希值;

所述通用区根据接收到的权限数据先后顺序,按序存储所述多项权限数据;

所述用户服务器确认所述多项权限数据全部发送完毕后,所述用户服务器向安全区通信接口发送权限验证命令,所述权限验证命令中包含所述多项权限数据,并标明所述用户服务器向所述通用区发送所述多项权限数据时的发送顺序;

所述安全区接收并存储所述多项权限数据后,所述安全区处理器生成一个随机序列,所述随机序列指示对通用区接收到的多项权限数据进行重排,所述安全区处理器将所述随机序列发送给所述通用处理器;

所述通用处理器根据所述随机序列对接收到的多项权限数据进行重排后,生成请求权限验证矩阵,将所述请求权限验证矩阵发送至安全处理器;

所述安全处理器采用相同的方式对多项权限数据进行重排并计算权限验证矩阵,并与通用处理器发送的请求权限验证矩阵进行比较,当所述权限验证矩阵和请求权限验证矩阵相同时,允许通用处理器对请求访问和更新的特权资源的区块进行访问和更新,同时打开授权许可期间定时器;

所述通用处理器判断对所述特权资源的更新完成时,向用户服务器返回更新完成信令。

2.如权利要求1所述方法,其特征在于,所述SoC包括通用区和安全区,其中所述通用区中包含通用处理器、通用存储区、通用通信接口,所述通用处理器用于在通用区中执行数据处理功能,所述通用存储区用于存储非特权数据,所述通用通信接口用于在通用区进行外部通信;所述安全区中包含安全处理器、安全存储区和安全通信接口,所述安全处理器用于在安全区中执行数据处理功能,所述安全存储区用于存储特权数据,所述安全通信接口用于在安全区进行外部通信;所述通用处理器通过安全通道接口与所述安全处理器进行安全数据通信。

3.如权利要求1所述的方法,其特征在于,所述服务器根据所述应用程序的信息,所述请求访问并更新的资源内容,以及设定的对所述请求访问并更新的资源内容的修改许可确定是否许可所述调用请求;

其中,所述用户服务器中存储有应用程序信息库,所述应用程序信息库中包含已知的

应用程序的可信信息状态，所述可信信息状态根据应用程序供应商的信用状态和所述应用程序的历史异常记录信息。

4.如权利要求1所述的方法，其特征在于，所述依次向通用区通信接口发送顺序随机的多项权限数据包括：

用户服务器发送一项权限信息数据后，接收到通用区返回的ACK信号后，再发送下一项权限信息数据，以保证通用区的接收顺序与发送顺序一致；所述通用区根据接收到的权限数据先后顺序，按序存储所述多项权限数据。

5.如权利要求1所述的方法，其特征在于，所述通用处理器根据所述随机序列对接收到的多项权限数据进行重排后生成请求权限验证矩阵具体如下：

假设所述用户服务器向所述通用区发送的权限数据为N项，排列成一个N维X向量，所述X向量为一个$1 \times N$维向量，通用处理器按照安全处理器发送的随机序列进行重排后得到重排后的X'向量，所述X'向量为一个$1 \times N$维向量；所述请求权限验证矩阵$M = X^T X'$，所述请求权限验证矩阵M为一个$N \times N$维的矩阵。

6.如权利要求1或5所述的方法，其特征在于，所述安全处理器采用相同的方式对多项权限数据进行重排并计算权限验证矩阵具体如下：

假设所述用户服务器向所述通用区发送的权限数据为N项，所述安全处理器将权限验证命令，并将所述权限验证命令中包含所述多项权限数据按照所述用户服务器向所述通用区发送所述多项权限数据时的发送顺序进行恢复，形成一个N维Y向量；

所述安全处理器根据所述随机序列进行重排后得到重排后的Y'向量，所述Y'向量为一个$1 \times N$维向量；

所述权限验证矩阵$P = Y^T Y'$，所述权限验证矩阵P为一个$N \times N$维的矩阵；

所述安全处理器将所述权限验证矩阵P与通用处理器发送的请求权限验证矩阵M进行比较，判断$P = M$时，允许通用处理器对请求访问和更新的特权资源的区块进行访问和更新。

7.如权利要求1所述的方法，其特征在于，

所述用户服务器接收到更新完成信令后，通知所述安全区终止本次安全会话，并清除本次会话的所有权限数据信息；

所述权限数据信息包括接收到的权限数据和生成的权限验证矩阵。

8.如权利要求7所述的方法，其特征在于，所述用户服务器接收到更新完成信令后，通知所述安全区终止本次安全会话之后还包括：

所述用户服务器通知安全区上传本次更新的特权资源区块的内容，并覆盖用户服务器中存储的特权资源区块的内容。

9.如权利要求1所述的方法，其特征在于，当所述授权许可期间定时器归0时，所述安全处理器主动终止安全会话，并向所述用户服务器发送配置更新异常指示。

10.如所述权利要求9所述的方法，其特征在于，

所述用户服务器接收所述配置更新异常指示后，向安全区发起恢复指示，所述恢复指示中包含本次会话中请求访问并更新的特权资源对应区块的备份内容，所述备份内容为发起本次更新前安全区中对应区块的内容。

一种基于SoC的物联网终端配置更新方法

技术领域

[0001] 本发明属于计算机技术领域，尤其涉及一种基于SoC的物联网终端配置更新方法。

背景技术

[0002] 随着5G和物联网技术的快速发展和普及，物联网设备的应用场景越来越广泛，在一些应用场景下，物联网终端的设备和信息安全非常重要，物联网终端的片上系统通常出厂时被设置为安全状态，此时通用处理器(属于SoC非特权模块)不允许访问芯片内部的特权资源。

[0003] 但是在实际应用中，对于安全状态的片上系统，通用处理器在运行一些程序时，需要访问芯片内的某些特权资源，有可能会对特权资源进行一些配置上的更新，使得这些程序得以正常运行。在这样的情形下，如何保证这些程序在运行时，不会访问多余不需要的特权数据，以及如何防止这些程序对特权数据做过分的改正更新，是现有阶段需要考量的。

发明内容

[0004] 针对上述现有技术中存在的缺陷，本发明提供一种基于SoC的物联网终端配置更新方法，应用于片上系统SoC，所述SoC包括通用区和安全区，其中所述通用区中包含通用处理器、通用存储区、通用通信接口，所述安全区中包含安全处理器、安全存储区和安全通信接口，所述方法包括：

[0005] 通用处理器执行应用程序时检测到所述应用程序请求访问并更新安全区存储区的特权资源；

[0006] 所述通用处理器调用通用通信接口向用户服务器发起调用请求，所述调用请求中包括请求访问并更新的资源内容，以及所述应用程序的信息；

[0007] 所述用户服务器接收调用请求，所述用户服务器确定许可调用请求后向通用区通信接口发送许可调用请求指令，否则发送拒绝调用请求指令；

[0008] 所述通用区接收到所述许可调用请求指令后向用户服务器发送预备状态反馈；

[0009] 所述用户服务器在接收到所述预备状态反馈后，依次向通用区通信接口发送顺序随机的多项权限数据，所述多项权限数据包括：授权许可期间，所述请求访问并更新的特权资源对应的区块ID，所述每一请求访问并更新的特权资源对应的区块的哈希值；

[0010] 所述通用区根据接收到的权限数据先后顺序，按序存储所述多项权限数据；

[0011] 所述用户服务器确认所述多项权限数据全部发送完毕后，所述用户服务器向安全区通信接口发送权限验证命令，所述权限验证命令中包含所述多项权限数据，并标明所述用户服务器向所述通用区发送所述多项权限数据时的发送顺序；

[0012] 所述安全区接收并存储所述多项权限数据后，所述安全区处理器生成一个随机序列，所述随机序列指示对通用区接收到的多项权限数据进行重排，所述安全区处理器将所述随机序列发送给所述通用处理器；

[0013] 所述通用处理器根据所述随机序列对接收到的多项权限数据进行重排后，生成请

求权限验证矩阵，将所述请求权限验证矩阵发送至安全处理器；

[0014] 所述安全处理器采用相同的方式对多项权限数据进行重排并计算权限验证矩阵，并与通用处理器发送的请求权限验证矩阵进行比较，当所述权限验证矩阵和请求权限验证矩阵相同时，允许通用处理器对请求访问和更新的特权资源的区块进行访问和更新，同时打开授权许可期间定时器；

[0015] 所述通用处理器判断对所述特权资源的更新完成时，向用户服务器返回更新完成信令。

[0016] 其中，所述SoC包括通用区和安全区，其中所述通用区中包含通用处理器、通用存储区、通用通信接口，所述通用处理器用于在通用区中执行数据处理功能，所述通用存储区用于存储非特权数据，所述通用通信接口用于在通用区进行外部通信；所述安全区中包含安全处理器、安全存储区和安全通信接口，所述安全处理器用于在安全区中执行数据处理功能，所述安全存储区用于存储特权数据，所述安全通信接口用于在安全区进行外部通信；所述通用处理器通过安全通道接口与所述安全处理器进行安全数据通信。

[0017] 其中，所述服务器根据所述应用程序的信息，所述请求访问并更新的资源内容，以及设定的对所述请求访问并更新的资源内容的修改许可确定是否许可所述调用请求；

[0018] 其中，所述用户服务器中存储有应用程序信息库，所述应用程序信息库中包含已知的应用程序的可信信息状态，所述可信信息状态根据应用程序供应商的信用状态和所述应用程序的历史异常记录信息。

[0019] 其中，所述依次向通用区通信接口发送顺序随机的多项权限数据包括：

[0020] 用户服务器发送一项权限信息数据后，接收到通用区返回的ACK信号后，再发送下一项权限信息数据，以保证通用区的接收顺序与发送顺序一致；所述通用区根据接收到的权限数据先后顺序，按序存储所述多项权限数据。

[0021] 其中，所述通用处理器根据所述随机序列对接收到的多项权限数据进行重排后生成请求权限验证矩阵具体如下：

[0022] 假设所述用户服务器向所述通用区发送的权限数据为N项，排列成一个N维X向量，所述X向量为一个$1 \times N$维向量，通用处理器按照安全处理器发送的随机序列进行重排后得到重排后的X'向量，所述X'向量为一个$1 \times N$维向量；所述请求权限验证矩阵$M = X^T X'$，所述请求权限验证矩阵M为一个$N \times N$维的矩阵。

[0023] 其中，所述安全处理器采用相同的方式对多项权限数据进行重排并计算权限验证矩阵具体如下：

[0024] 假设所述用户服务器向所述通用区发送的权限数据为N项，所述安全处理器将权限验证命令，并将所述权限验证命令中包含所述多项权限数据按照所述用户服务器向所述通用区发送所述多项权限数据时的发送顺序进行恢复，形成一个N维Y向量；

[0025] 所述安全处理器根据所述随机序列进行重排后得到重排后的Y'向量，所述Y'向量为一个$1 \times N$维向量；

[0026] 所述权限验证矩阵$P = Y^T Y'$，所述权限验证矩阵P为一个$N \times N$维的矩阵；

[0027] 所述安全处理器将所述权限验证矩阵P与通用处理器发送的请求权限验证矩阵M进行比较，判断$P = M$时，允许通用处理器对请求访问和更新的特权资源的区块进行访问和更新。

[0028] 其中，所述用户服务器接收到更新完成信令后，通知所述安全区终止本次安全会话，并清除本次会话的所有权限数据信息；

[0029] 所述权限数据信息包括接收到的权限数据和生成的权限验证矩阵。

[0030] 其中，所述用户服务器接收到更新完成信令后，通知所述安全区终止本次安全会话之后还包括：

[0031] 所述用户服务器通知安全区上传本次更新的特权资源区块的内容，并覆盖用户服务器中存储的特权资源区块的内容。

[0032] 其中，当所述授权许可期间定时器归0时，所述安全处理器主动终止安全会话，并向用户服务器发送配置更新异常指示。

[0033] 其中，所述用户服务器接收所述配置更新异常指示后，向安全区发起恢复指示，所述恢复指示中包含本次会话中请求访问并更新的特权资源对应区块的备份内容，所述备份内容为发起本次更新前安全区中对应区块的内容。

[0034] 与现有技术相比，通用区应用在获得可信许可后，根据用户服务器发送的各项权限数据以及安全区发送的随机序列，生成请求权限验证矩阵向安全区验证后请求对应的特权资源块。通过本发明的方法使得通用区不会访问多余不需要的特权数据，也可以防止通用区程序对特权数据做过分的改正更新。

附图说明

[0035] 通过参考附图阅读下文的详细描述，本公开示例性实施方式的上述以及其他目的、特征和优点将变得易于理解。在附图中，以示例性而非限制性的方式示出了本公开的若干实施方式，并且相同或对应的标号表示相同或对应的部分，其中：

[0036] 图1是示出根据本发明实施例的一种基于SoC的物联网终端配置更新方法流程图。

具体实施方式

[0037] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0038] 在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制

本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义，“多种”一般包含至少两种。

[0039] 应当理解，尽管在本发明实施例中可能采用术语第一、第二、第三等来描述……，但这些……不应限于这些术语。这些术语仅用来将……区分开。例如，在不脱离本发明实施例范围的情况下，第一……也可以被称为第二……，类似地，第二……也可以被称为第一……。

[0040] 应当理解，本文中使用的术语“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0041] 取决于语境，如在此所使用的词语“如果”、“若”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地，取决于语境，短语“如果确定”或“如果检测(陈述的条件或事件)”可以被解释成为“当确定时”或“响应于确定”或“当检测(陈述的条件或事件)时”或“响应于检测(陈述的条件或事件)”。

[0042] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的商品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种商品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的商品或者装置中还存在另外的相同要素。

[0043] 下面结合附图详细说明本发明的可选实施例。

[0044] 实施例一、

[0045] 如图1所示，本发明公开了一种基于SoC的物联网终端配置更新方法，应用于片上系统SoC，所述SoC包括通用区和安全区，其中所述通用区中包含通用处理器、通用存储区、通用通信接口，所述安全区中包含安全处理器、安全存储区和安全通信接口，所述方法包括：

[0046] 通用处理器执行应用程序时检测到所述应用程序请求访问并更新安全区存储区的特权资源；

[0047] 所述通用处理器调用通用通信接口向用户服务器发起调用请求，所述调用请求中包括请求访问并更新的资源内容，以及所述应用程序的信息；

[0048] 所述用户服务器接收调用请求，所述用户服务器确定许可调用请求后向通用区通信接口发送许可调用请求指令，否则发送拒绝调用请求指令；

[0049] 所述通用区接收到所述许可调用请求指令后向用户服务器发送预备状态反馈；

[0050] 所述用户服务器在接收到所述预备状态反馈后，依次向通用区通信接口发送顺序随机的多项权限数据，所述多项权限数据包括：授权许可期间，所述请求访问并更新的特权资源对应的区块ID，所述每一请求访问并更新的特权资源对应的区块的哈希值；

[0051] 所述通用区根据接收到的权限数据先后顺序，按序存储所述多项权限数据；

[0052] 所述用户服务器确认所述多项权限数据全部发送完毕后，所述用户服务器向安全区通信接口发送权限验证命令，所述权限验证命令中包含所述多项权限数据，并标明所述用户服务器向所述通用区发送所述多项权限数据时的发送顺序；

[0053] 所述安全区接收并存储所述多项权限数据后，所述安全区处理器生成一个随机序

列，所述随机序列指示对通用区接收到的多项权限数据进行重排，所述安全区处理器将所述随机序列发送给所述通用处理器；

[0054] 所述通用处理器根据所述随机序列对接收到的多项权限数据进行重排后，生成请求权限验证矩阵，将所述请求权限验证矩阵发送至安全处理器；

[0055] 所述安全处理器采用相同的方式对多项权限数据进行重排并计算权限验证矩阵，并与通用处理器发送的请求权限验证矩阵进行比较，当所述权限验证矩阵和请求权限验证矩阵相同时，允许通用处理器对请求访问和更新的特权资源的区块进行访问和更新，同时打开授权许可期间定时器；

[0056] 所述通用处理器判断对所述特权资源的更新完成时，向用户服务器返回更新完成信令。

[0057] 其中，用户服务器和安全区都是处于安全可信状态，用户服务器可以和所服务的多个物联网终端的安全区处于同样的安全可信级别，从某种程度上，可以理解为用户服务器和单个的安全区形成只有两个成员区块链的机制，用户服务器和每个安全区都形成一条这样的链。本申请中，用户服务器中保存有所有安全区的特权资源信息，当安全区的特权资源进行更新的时候，服务器也同样对安全区的特权资源进行更新，作为安全区资源的一个备份，服务器中也同样按照区块分别存储这些特殊资源，因此当通用区向用户服务器请求特定特权资源时，用户服务器就可以计算这些区块对应内容的哈希值，将各区块的ID、区块对应的哈希值和授权许可期间作为权限数据发送给通用区。

[0058] 在某一可选实施例中，所述SoC包括通用区和安全区，其中所述通用区中包含通用处理器、通用存储区、通用通信接口，所述通用处理器用于在通用区中执行数据处理功能，所述通用存储区用于存储非特权数据，所述通用通信接口用于在通用区进行外部通信；所述安全区中包含安全处理器、安全存储区和安全通信接口，所述安全处理器用于在安全区中执行数据处理功能，所述安全存储区用于存储特权数据，所述安全通信接口用于在安全区进行外部通信；所述通用处理器通过安全通道接口与所述安全处理器进行安全数据通信。

[0059] 在某一可选实施例中，所述用户服务器根据所述应用程序的信息，所述请求访问并更新的资源内容，以及设定的对所述请求访问并更新的资源内容的修改许可确定是否许可所述调用请求；

[0060] 在某一可选实施例中，所述用户服务器中存储有应用程序信息库，所述应用程序信息库中包含已知的应用程序的可信信息状态，所述可信信息状态根据应用程序供应商的信用状态和所述应用程序的历史异常记录信息。

[0061] 其中，应用程序的历史异常记录信息可以是其他设备上报的更新异常、或者是超出权限的修改等信息。

[0062] 在某一可选实施例中，所述依次向通用区通信接口发送顺序随机的多项权限数据包括：

[0063] 用户服务器发送一项权限信息数据后，接收到通用区返回的ACK信号后，再发送下一项权限信息数据，以保证通用区的接收顺序与发送顺序一致；所述通用区根据接收到的权限数据先后顺序，按序存储所述多项权限数据。

[0064] 在某一可选实施例中，所述通用处理器根据所述随机序列对接收到的多项权限数

据进行重排后生成请求权限验证矩阵具体如下：

[0065] 假设所述用户服务器向所述通用区发送的权限数据为N项，排列成一个N维X向量，所述X向量为一个$1 \times N$维向量，通用处理器按照安全处理器发送的随机序列进行重排后得到重排后的X'向量，所述X'向量为一个$1 \times N$维向量；所述请求权限验证矩阵$M = X^T X'$，所述请求权限验证矩阵M为一个$N \times N$维的矩阵。

[0066] 在某一可选实施例中，所述安全处理器采用相同的方式对多项权限数据进行重排并计算权限验证矩阵具体如下：

[0067] 假设所述用户服务器向所述通用区发送的权限数据为N项，所述安全处理器将权限验证命令，并将所述权限验证命令中包含所述多项权限数据按照所述用户服务器向所述通用区发送所述多项权限数据时的发送顺序进行恢复，形成一个N维Y向量；

[0068] 所述安全处理器根据所述随机序列进行重排后得到重排后的Y'向量，所述Y'向量为一个$1 \times N$维向量；

[0069] 所述权限验证矩阵$P = Y^T Y'$，所述权限验证矩阵P为一个$N \times N$维的矩阵；

[0070] 所述安全处理器将所述权限验证矩阵P与通用处理器发送的请求权限验证矩阵M进行比较，判断$P = M$时，允许通用处理器对请求访问和更新的特权资源的区块进行访问和更新。

[0071] 在某一实施例中，假如通用区请求的特殊资源对应的区块为2个，分别为区块A、区块B，区块A、区块B对应的ID为ID_A、ID_B，区块A、B对应的哈希值为Hash_A、Hash_B，用户服务器分配给通用区的授权许可期间为DurationAB，可见用户服务器向通用区发送的权限数据项数为5项，在实际使用中，请求的特殊资源对应的区块可以是大于1的任意个数。

[0072] 用户服务器随机将这5项权限数据发送给通用区，并在通用区接收到每一项返回ACK后再发送下一项。例如，按照[ID_A,ID_B,DurationAB,Hash_A,Hash_B]发送给通用区，通用区按照这个顺序存储这个数列，记为X=[ID_A,ID_B,DurationAB,Hash_A,Hash_B]。

[0073] 同时，用户服务器也将这些参数的值发送给安全区，这个发送也可以通过指示的方式，也可以直接将结果发送给安全区，例如，用户服务器可以直接告知安全区请求的特权资源内容，由安全区自行确定区块并计算hash值，或者将区块ID发送给安全区，安全区根据区块ID计算hash值，或者直接将区块ID和hash值发送给安全区，具体采用哪种方式，可以根据物联网终端的安全区处理器的计算能力来决定。同时用户服务器需要将授权许可期间发

送给安全区，这一授权许可期间是用户服务器根据物联网终端的处理能力、处理数据量大小和存储的历史信息参考和估计的该物联网终端需要访问并更新特权资源全过程的时间；

[0074] 假如用户服务器向安全区发送已经计算好的全部参数，在这些参数中标明用户设备向通用区发送这些参数的序列，例如向安全区发送[1,ID_A]、[4,Hash_A]、[2,ID_B]、[5,Hash_B]、[3,DurationAB]，序号比如可以包含在数据包的包头中，数据包头中还可以包括总的数据包个数，个数5也可以指示在包头中，比如[1,5,ID_A]。

[0075] 安全区接收到这些数据包以后，按照通用区的接收顺序把数据包内容提取恢复成Y，Y=[ID_A,ID_B,DurationAB,Hash_A,Hash_B]。

[0076] 安全区生成一个随机序列，这个随机序列是用于对通用区存储的数据进行重排的，例如这个随机序列为{4,5,3,1,2}，安全区处理器将这个随机序列发送个通用区。

[0077] 通用区处理器接收安全处理器通过安全通道发送的这个随机序列，按照这个随机序列对存储的权限数据序列进行重排，重排结果为X'=[Hash_A,Hash_B,DurationAB, ID_A,ID_B]。同样地，安全区处理器也按照自己生成的序列对存储的Y序列进行重排生成Y'，Y'和X'应当是相同的序列。

[0078] 最后，请求权限验证矩阵$M = X^T X'$和权限验证矩阵$P = Y^T Y'$，在本实施例中，M、P都应该是一个5×5维的矩阵。生成请求权限验证矩阵还可以采用其他算法，如安全区还可以确定一个随机数，也发送给通用区，该随机数可以是整数，也可以是浮点数，用这个随机数对$X^T X'$进行倍乘，或者是令$M = X'^T X$，也可以生成一个5×5维的矩阵，都是可行的，使用验证矩阵而不是数列的目的，是可以通过安全区的一个随机生成并在安全通道发送的方式使得第三方获得用户服务器发送的数据还不能获取安全区的特权资源数据，避免通用区被第三方冒用权限获得安全区的特权资源数据，使用矩阵数据相比于数列来说也使得这一验证结果被破译的可能性更低，使得这一更新过程更加安全。

[0079] 通用区将请求权限验证矩阵发送给安全区，在安全区中对两者是否完全相等进行验证。

[0080] 通过这一方式进行安全验证，不仅需要验证通用区运行的程序的可靠性，还可以校验用户服务器和通用区的通信可靠性，还需要验证安全区和通用区通信的可靠性，保证了各个环节通信的绝对可靠，防止第三方在这一过程的任何环节进行假冒身份篡改的可能性，还可以防止通用区程序对特权资源不必要的访问和更改，只允许其做必要的访问和更新，保证隐私数据的安全性。

[0081] 在某一可选实施例中，所述用户服务器接收到更新完成信令后，通知所述安全区终止本次安全会话，并清除本次会话的所有权限数据信息；

[0082] 所述权限数据信息包括接收到的权限数据和生成的权限验证矩阵。

[0083] 在某一可选实施例中，所述用户服务器接收到更新完成信令后，通知所述安全区

终止本次安全会话之后还包括：

[0084] 所述用户服务器通知安全区上传本次更新的特权资源区块的内容，并覆盖用户服务器中存储的特权资源区块的内容。

[0085] 在某一可选实施例中，当所述授权许可期间定时器归0时，所述安全处理器主动终止安全会话，并向服务器发送配置更新异常指示。

[0086] 在某一可选实施例中，所述用户服务器接收所述配置更新异常指示后，向安全区发起恢复指示，所述恢复指示中包含本次会话中请求访问并更新的特权资源对应区块的备份内容，所述备份内容为发起本次更新前安全区中对应区块的内容。

[0087] 在某一实施例中，用户服务器和安全区中都存储有相同的特权资源信息，并且用户服务器记录每一次更新的特权资源信息的修改内容和修改来源，用户服务器定期进行安全漏洞扫描，当发现不安全或可疑的漏洞时，定位到对应的修改来源，快速确定可疑修改的来源程序、和物联网终端。用户服务器向物联网终端的安全区发起恢复请求撤回该次修改的所有更新内容到之前的版本，并且在用户服务器中的应用程序信息库对这次可疑修改的来源的应用程序进行标注，如假如黑名单，或者进行警示标记，等等操作，后续就可以对该应用程序请求请求对该物联网设备或者和用户服务器服务的其他物联网设备进行配置更新时进行权限限制等操作。

[0088] 与现有技术相比，通用区应用在获得可信许可后，根据用户服务器发送的各项权限数据以及安全区发送的随机序列，生成请求权限验证矩阵向安全区验证后请求对应的特权资源块。通过本发明的方法使得通用区不会访问多余不需要的特权数据，也可以防止通用区程序对特权数据做过分的改正更新。

[0089] 需要说明的是，本公开上述的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本公开中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本公开中，计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读信号介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：电线、光缆、RF(射频)等等，或者上述的任意合适的组合。

[0090] 上述计算机可读介质可以是上述电子设备中所包含的；也可以是单独存在，而未装配入该电子设备中。

[0091] 可以以一种或多种程序设计语言或其组合来编写用于执行本公开的操作的计算机程序代码，上述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C+

+,还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0092] 附图中的流程图和框图,图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0093] 描述于本公开实施例中所涉及到的单元可以通过软件的方式实现,也可以通过硬件的方式来实现。其中,单元的名称在某种情况下并不构成对该单元本身的限定。

[0094] 以上介绍了本发明的较佳实施方式,旨在使得本发明的精神更加清楚和便于理解,并不是为了限制本发明,凡在本发明的精神和原则之内,所做的修改、替换、改进,均应包含在本发明所附的权利要求概括的保护范围之内。

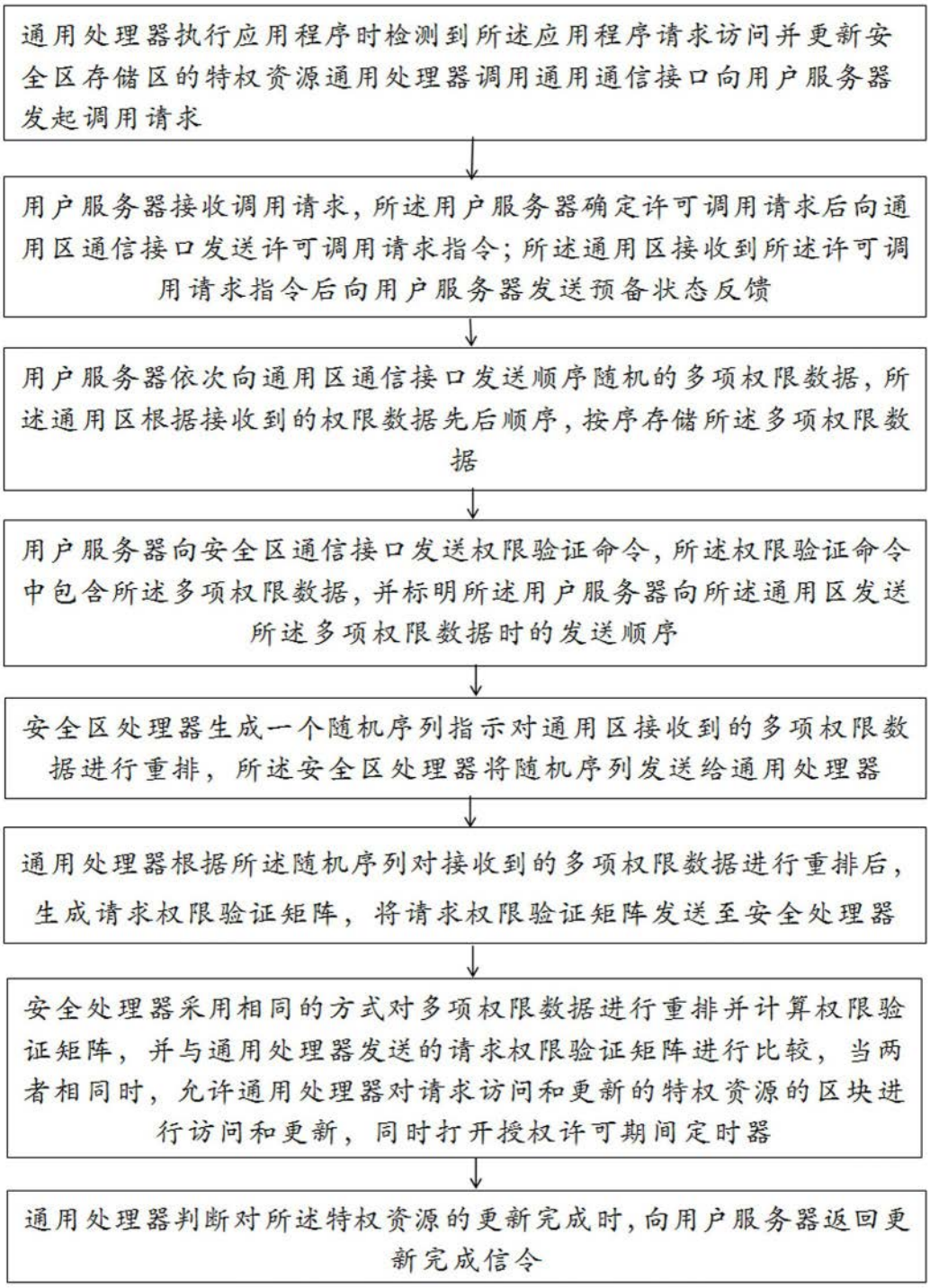

通用处理器执行应用程序时检测到所述应用程序请求访问并更新安全区存储区的特权资源通用处理器调用通用通信接口向用户服务器发起调用请求
用户服务器接收调用请求，所述用户服务器确定许可调用请求后向通用区通信接口发送许可调用请求指令；所述通用区接收到所述许可调用请求指令后向用户服务器发送预备状态反馈
用户服务器依次向通用区通信接口发送顺序随机的多项权限数据，所述通用区根据接收到的权限数据先后顺序，按序存储所述多项权限数据
用户服务器向安全区通信接口发送权限验证命令，所述权限验证命令中包含所述多项权限数据，并标明所述用户服务器向所述通用区发送所述多项权限数据时的发送顺序
安全区处理器生成一个随机序列指示对通用区接收到的多项权限数据进行重排，所述安全区处理器将随机序列发送给通用处理器
通用处理器根据所述随机序列对接收到的多项权限数据进行重排后，生成请求权限验证矩阵，将请求权限验证矩阵发送至安全处理器
安全处理器采用相同的方式对多项权限数据进行重排并计算权限验证矩阵，并与通用处理器发送的请求权限验证矩阵进行比较，当两者相同时，允许通用处理器对请求访问和更新的特权资源的区块进行访问和更新，同时打开授权许可期间定时器
通用处理器判断对所述特权资源的更新完成时，向用户服务器返回更新完成信令

图 1